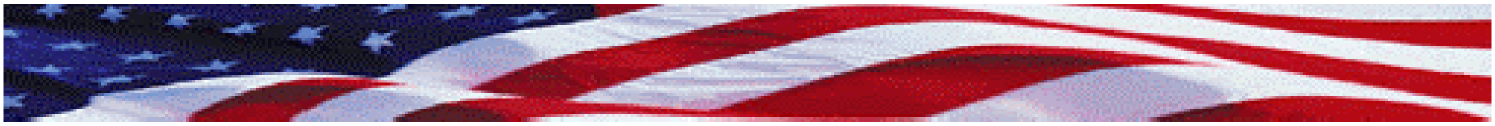
e-Authentication

Making trust possible



e-Authentication Initiative
Program Overview

For governments to expand their electronic service delivery capabilities and truly become "e-governments," an authentication framework is required. The e-Authentication Initiative provides the necessary technical architecture.

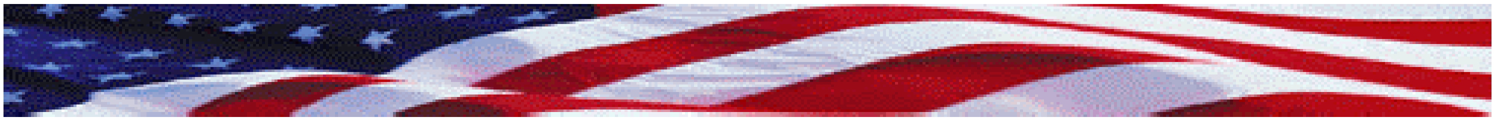
e-Authentication:

- Provides common authentication services in support of Federal e-Government (e-Gov) programs
- Associates level of assurance to authentication technology
- Promotes interoperability and standards for Electronic Credential Providers (ECPs)

The e-Authentication Gateway's core principles are:

- The e-Authentication Gateway will not issue credentials. Credentials will be issued by authorized ECPs.
- The e-Authentication Gateway accepts electronic credentials from individuals and applications (users) requesting services from e-Gov applications and determines the validity of the credential presented.
- The e-Gov applications are responsible for managing all access controls and permissions related to the services being requested by the users.
- The e-Gov applications are responsible for determining their requirements for unique user information to manage access controls and permissions.
- Each e-Gov application owner will define specific assurance level requirements based on the defined levels of assurance in the OMB and NIST guideline documents (see http://www.cio.gov/eauthentication)
- Applications requiring lower levels of assurance for authentication of identity will grant access based on validation of credentials issued at a higher level of assurance.
- Once a user's credential has been validated by the e-Authentication Gateway for access to one e-Gov application, access to another e-Gov application will not require re-validation of the credential, if the authentication of identity requirements for the second application are equal to or less than those of the first application (e.g., single sign-on), taking into account timeout and refresh policies.
- The application may request additional information from the user requesting services in order to grant access. An application may grant access at a higher level of assurance than that associated with the user's credential for use with that local application only. This does not change the level of assurance for the user's credential when access and services from another application are requested by that user.
- The e-Authentication Gateway handles Private Consumer Information (PCI) in accordance with OMB Privacy Management Guidelines. The definition and implementation of the PCI Gateway function of the e-Authentication Gateway will be based on those guidelines.

(continued)



The e-Authentication Gateway:

- Validates electronic credentials on behalf of applications
- Provides a single interface between the agency application (AA) and the ECP
- Does not maintain user personal information or user behavior and profiles

The ECPs will provide user identity management services including:

- Collecting and verifying identity information from the user
- Issuing and managing user credentials
- Defining the protocols supported for validation of their credentials
- Responding to credential status information/validation requests received from the e-Authentication technical architecture
- Storing user information

The e-Authentication technical architecture maintains a list of approved ECPs and the level of assurance of the associated credential they issue based on OMB guidance. In certain cases, a user may have multiple electronic credentials, at the same or different levels. If the user obtains higher-level credentials, the lower level credentials are still useable where appropriate.

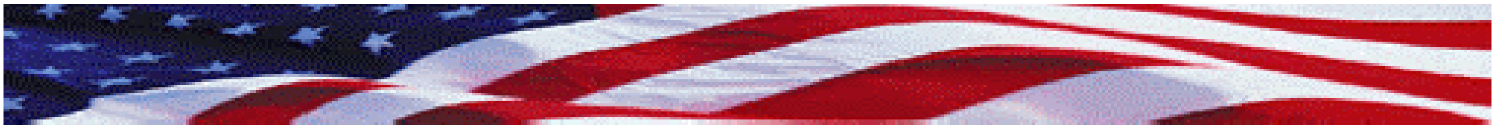
Agency application interoperability with e-Authentication can be conducted as follows:

- Programmatic
  - Determine identity authentication requirements
    - Risk assessment tools available, such as (e-Authentication Risk and Requirements Assessments (e-RA)
  - Determine resource protection policies for authorization management
- Technical
  - Meet with e-Authentication technical architecture development team to identify unique interoperability requirements
  - Determine integration requirements to complete interface from e-Authentication to backend business processes
- Complete integration testing with Initial Operating Capability (IOC) e-Authentication Gateway development test-bed
- Integrate with “on-line” IOC e-Authentication Gateway following successful testing

Agencies that want to use the IOC e-Authentication Gateway’s authentication services are required to execute a Memorandum of Agreement (MOA) with the e-Authentication Initiative.

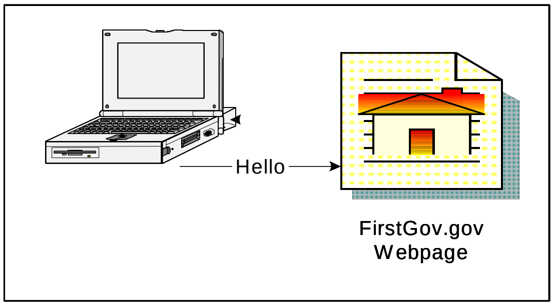
e-Authentication

Making trust possible

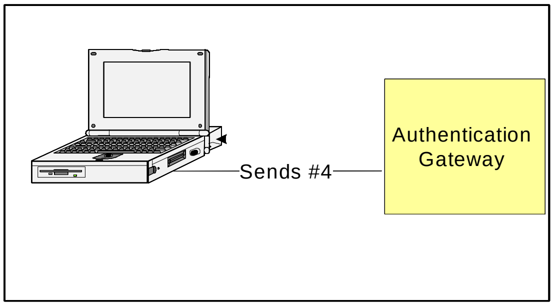


e-Authentication Gateway Process Flow

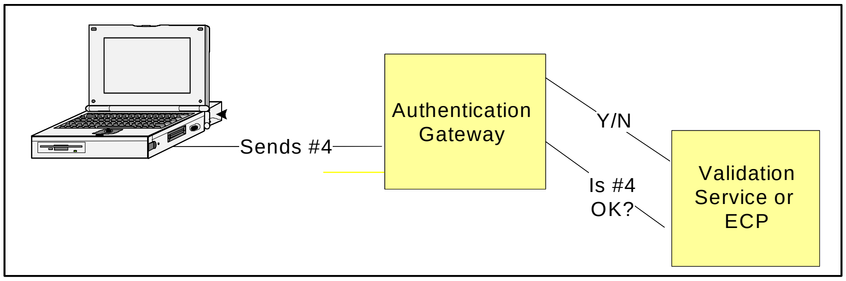
The following diagrams illustrate a typical Initial Operating Capability (IOC) e-Authentication Gateway user session at a high level. It assumes that the user initially discovers the desired e-Gov application via a portal, such as FirstGov.gov:



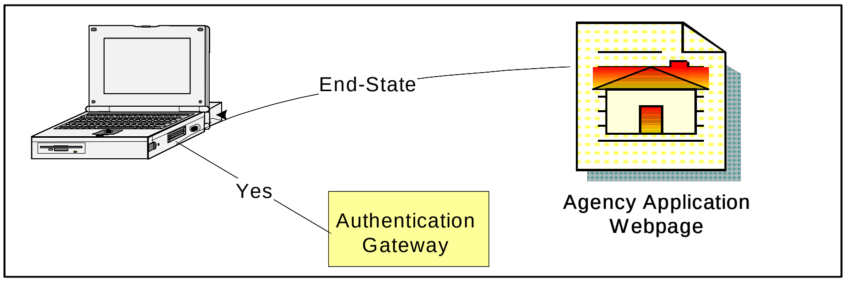
Step 1. User goes to FirstGov web portal and selects e-Gov application service



Step 2.. User is re-directed to e-Authentication Gateway to present credential required by application.



Step 3. e-Authentication Gateway validates user's credential

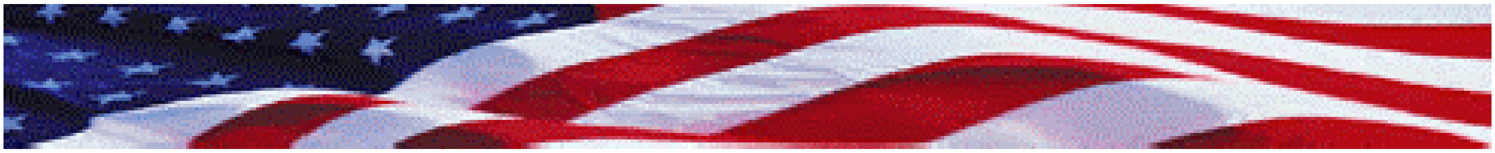


Step 4. If user's credential is valid, user is re-directed to agency application for services

(continued)

e-Authentication

Making trust possible



Interim e-Authentication Gateway Process Flow

Step 1: A user comes to the FirstGov web portal:

- At the portal, the user selects an e-Gov application such as one from United States Department of Agriculture-National Finance Center (USDA-NFC)

Step 2: Based on the application and service selected by the user:

- Before the user begins interacting with the application, the portal queries the IOC e-Authentication Gateway for USDA-NFC's authentication level of assurance requirements (e.g., must be Assurance Level 4 in the example.) (The gateway retrieves the authentication level requirements from decentralized lists and databases)
- The gateway queries the user for a credential matching or exceeding the required level
- The user's credential is presented to the gateway
- If the user does not have a digital credential of the appropriate level, the user is denied access to the application and is re-directed back to the portal for further information about how to obtain a credential at the required level of assurance

Step 3: The user's credential is validated:

- The IOC e-Authentication Gateway validates the user's electronic credential via a validation service or by performing a query directly to the ECP
- If the electronic credential is valid, the IOC e-Authentication Gateway's response to this effect is conveyed to the application and the user's browser is updated with a non-persistent cookie
- If the credential is not valid, the user is informed that their electronic credential has been rejected and is provided with a link to be re-directed to the web portal

Step 4: If the credential is valid, the user is re-directed to the agency application to obtain desired services.

After the user has been initially authenticated by the IOC e-Authentication Gateway, the user may select another application. The other application will query the IOC e-Authentication Gateway for session and validation information and proceed to grant access to the user, according to its own access controls and privilege management policies. The user will not have to be re-authentication if this occurs.